Svakarma Finance Pvt Ltd

KYC-AML Policy

1. Background

Svakarma Finance Private Limited [the Company/Svakarma] is engaged in the business of lending to micro, small and medium enterprises (MSMEs) in sectors such as manufacturing, retail trading, food / agriculture and allied services, textiles, rural livelihoods, water & sanitation, etc.

Svakarma offers financing solutions that closely follow the cash flow cycle of our customer's business through an efficient product delivery model coupled with a branch presence in close proximity with the MSME clusters. The ultimate target beneficiary of Svakarma is the underserved participants / consumers in the focus sectors where our involvement **will make a measurable positive impact.**

Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-money Laundering (AML) standards and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures is formulated and put in place with the approval of the Board.

Accordingly, in compliance with the Master Directions/Guidelines issued by RBI from time to time, the KYC & AML policy of the Company as approved by the Board of Directors of the Company is as given below. This policy is applicable to all categories of products and services offered by the Company.

2. Objective:

Objective of this Policy is to prevent Svakarma being used, intentionally or unintentionally by criminal elements for money laundering activities. The Policy also mandates making reasonable efforts to determine the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

3. Definition of a Customer

For the purpose of KYC policy, a 'Customer' may be defined as an entity which is engaged in a financial transaction or activity with the Company. The definition also includes any other person / entity on whose behalf the said transaction or activity is being conducted as well as normally non active parties to such transactions like the co-borrowers and guarantors.

4. Customer Acceptance Policy (CAP)

The Company shall follow the following norms while accepting and dealing with its customers.

Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of

the customer and his clients, mode of payments, volume of turnover, social and financial status, etc. to enable the categorization of the customers into low, medium and high risk.

1. Svakarma will through a detailed Personal Discussion (PD) process collect information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing customer profile, the Company will seek only such information from the customer that is relevant to the risk categorisation and is not intrusive. The customer profile will be a confidential document and details contained therein will not be divulged for cross selling or any other purpose.
2. The adoption of customer due diligence & acceptance policy, as well as its implementation should not be so restrictive as to result in denial of financial services to the general public, especially those, who are financially or socially disadvantaged.
3. The Company shall carry out full-scale customer due diligence (CDD) before opening a loan account. When the true identity of the account holder is not known, the Company shall not enter into any transaction with such an entity

5. Customer Identification Procedure (CIP)

Customer identification implies using reliable and independent source of documents, data or information for establishing the identity of the customer; and where the customer is not an individual then the enterprise's identity. This is to ensure that the customer is not a fictitious person. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each customer and the purpose of the intended nature of business relationship. An effective Customer Identification Program ("CIP") is an important part of the effort by the Company to know its customers. The Company's CIP, is integrated into the AML (Anti Money Laundering) program for the Company in terms of the Prevention of Money Laundering Act, 2002 (PMLA), and the relevant rules notified there under which contains provisions requiring the business processes to:

1. Verify the identity of any Person transacting with the Company to the extent reasonable and practicable;
2. Maintain records of the information used to verify a customer's identity, including name, address and other identifying information;
3. Consult lists of known or suspected terrorists or terrorist organizations and available negative customer lists to determine whether a person opening an account or an existing customer appears on any such list. The same may be done through various KYC verification platforms such as world check, RCU checks etc)
4. The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence [EDD] on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

6. Customer Due Diligence (CDD) requirements

The Company shall take reasonable measures to ascertain and verify the true identity of all customers who transact with the Company. The Company shall design and implement specific due diligence standards and procedures that are appropriate given the nature of the respective businesses, customers and the associated risks. Such standards and procedures shall include, at a minimum, the following elements:

a) Identification

Unique identification codes will be used to identify all customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of customers. The Company shall implement procedures to obtain from each Customer, prior to transacting, the following information as may be relevant, to that business:

1. Name - procedures require business processes to use reasonable efforts to ensure that the name recorded on the Company systems are exactly the same as (and not merely similar to, or a variation of) the customer name that appears on any identifying documentation reviewed in connection with the loan; In case of mismatch in name of the Borrower with the Documents, a Declaration is taken along with the proof such as marriage certificate, bank statement etc.
2. Latest Photograph- Passport size photo of the Customer.
3. Date of birth / Date of incorporation – for individuals / other than individuals (such as a corporation, partnership, or trust);
4. Address (along with documentary proof thereof) – (a) For individuals- residential or business address (b) for other than individuals- the principal place of business, local office, or other physical location;
5. Telephone/Fax number/E-mail ID;
6. Identification number: Valid PAN or Form 60 as per IT Rules 1962; passport number and country of issuance; letter issued by Unique Identification Authority of India containing AADHAAR number passport or any other government issued document evidencing nationality or residence and bearing a photograph. When opening an account for a person (other than an individual) that does not have an identification number, the business process must request alternative government issued documentation certifying the existence of the business or enterprise;

The Company shall ensure to redact or blackout the Aadhaar number in terms of Section 16 of Master Direction issued by RBI.

For a customer who has applied for, but has not received an identification number, loan may be sanctioned, but business process shall implement procedures to confirm that the application was filed before the loan is sanctioned to customer and to obtain the identification number within a reasonable period of time before/after disbursal of loan.

The list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company is given as Annexure-3 to this policy. These are appropriately covered in the credit policy and communicated to the credit approving authorities.

For proprietary concerns, the Company will collect any two documents from the list given in Annexure-3. Only where the Company is satisfied that it is not possible for the customer to furnish two such documents; the Company will have the discretion to accept only one of those documents as activity proof. In such a situation, the Company will record the appropriate reason for accepting one document as identity proof.

In case of existing KYC compliant customers desirous of opening another account, the KYC process will be guided by relevant guidelines specified under **section j) "risk categorization**" of this policy.

b) Verification

The Company as a part of the credit policy will document and implement appropriate risk-based procedures designed to verify the true identity of its customers. Verification of customer identity should occur before transacting with the customer. Procedures for each business process shall describe acceptable methods of verification of customer identity, which may include verification through documents or non-documentary methods that are appropriate given the nature of the business process, the products and services provided and the associated risks.

1. Verification through documents: These documents may include, but are not limited to documents listed in Annexure-3 that can be accepted as proof of identity and address from customers across various products offered. These documents are appropriately covered in the credit policy. An independent screening of the KYC documents provided by the customer for its authenticity will also be done through specialized vendors.

   For customers operating under trust / nominee or fiduciary accounts, in addition to the documents as defined under Annexure -3, some additional checks are defined in Annexure 2. The customer verification processes will also be covered in detail in the credit policy.
2. Verification through non-documentary methods: These methods may include, but are not limited to:
   I. Contacting or visiting the customer;
   II. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a bureau / reporting agency, public database, and / or other source;
   III. Checking references with other financial institutions; suppliers and buyers of the prospective customer.
   IV. Obtaining a financial statement.

Where appropriate, the business process should implement additional verification procedures. Such verification procedures will be applicable where :

I. A person is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
II. The Svakarma representative is not familiar with the documents presented;
III. Where it is determined that identity verification is not possible through the submitted set of customer documents and
IV. If the business process cannot verify the identity of a non-individual entity, it may be necessary to obtain information about persons with authority or control over such an entity (including authorized signatories) in order to verify the customer entity's identity.

c) Resolution of Discrepancies

Each business process shall document & implement procedures to resolve information discrepancies and to decline or cease to do business with a customer where it cannot form a reasonable belief that it knows the true identity of such customer and / or cannot adequately complete necessary due diligence. These procedures should include identification of responsible decision makers and escalation paths and detailed standards relating to what actions will be taken if a customer's identity cannot be adequately verified.

d) Reporting

The Company shall have a system of internal reporting of suspicious transactions, counterfeit transactions and cash transactions **greater than Rs.1 lakh**, (excluding loan closure payments) whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month.

"Suspicious transaction" means a transaction whether or not made in cash which, to a person acting in good faith:

I. Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
II. Appears to be made in circumstances of unusual or unjustified complexity; or
III. Appears to have no economic rationale or bonafide purpose or
IV. Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
V. Where the transactions are abandoned by customers on being asked to give some details or to provide documents

Further, the Principal officer shall furnish information of the above-mentioned transactions to the Director, Financial Intelligence Unit – India (FIU-IND) at the prescribed address in the formats prescribed in this regard including the electronic filing of reports.

Provided that where the Principal officer, has reason to believe that a single cash transaction or series of cash transactions integrally connected to each other are valued at greater than or **Rs.1 lakhs** (on cumulative monthly aggregate of basis) with a specific purpose of defeating the provisions of the PMLA regulations, principal officer shall furnish information in respect of such transactions to the Director – FIU within the prescribed time.

e) Records Retention

The Company shall document and implement appropriate procedures to retain records of KYC due diligence and anti-money laundering measures. The business process shall implement, at a minimum, the following procedures for retaining records:

(a) maintain all necessary records of transactions between the Company and the customer, both domestic and international, for at least five years from the date of transaction;

(b) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;

(c) make available the identification records and transaction data to the competent authorities upon request;

(d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

(e) maintain all necessary information in respect of transactions prescribed under PML Rule 3 to permit reconstruction of individual transaction, including the following:

i. the nature of the transactions;
ii. the amount of the transaction and the currency in which it was denominated;
iii. the date on which the transaction was conducted; and
iv. the parties to the transaction.

(f) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

(g) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

"Suspicious transaction" means a "transaction" as defined below, including an attempted transaction, whether made in cash or not, which, to a person acting in good faith:

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to not have economic rationale or bona-fide purpose; or
d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

f) CIP Notice

The Company shall implement procedures to ensure that customers are given adequate notice when the Company requests information / takes actions towards verifying their identity. Each business process shall determine the appropriate manner to deliver the notice, which shall be reasonably designed to ensure that the customer is able to view or is otherwise given such notice prior to account opening.

g) Existing Customer

The requirements of the earlier sections are not applicable to accounts opened by existing customers, provided that the business process has previously verified the identity of the customer and the business process continues to have a reasonable belief that it knows the true identity of the customer. Further, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the due diligence measures.

h) Enhanced Due Diligence [EDD]

The Company is primarily engaged in lending to micro, small and medium enterprises. It does not deal with such category of customers who could pose a potential high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The existing credit policy of the Company in respect of its businesses ensure that the Company is not transacting with such **high-risk customers/ restricted profiles**. The Company shall conduct EDD in connection with all customers or accounts that are deemed to be "potential high risk" and are determined to warrant enhanced scrutiny. Each

business process shall establish appropriate standards, methodology and procedures for conducting EDD, which shall involve additional steps beyond what is required by standard KYC due diligence. EDD shall be coordinated and performed by the Company, who may engage appropriate outside investigative services or consult appropriate third party databases when necessary. As a precautionary measure, Svakarma shall conduct dedupe for all the customers on global AML & CTF database like Worldcheck or any other similar software. Each business process shall establish procedures designed to refuse or discontinue customer relationships when the Company cannot adequately complete necessary EDD on the said customer. These procedures will also apply when the information received is deemed to have a significant adverse impact on Company's reputational risk.

The following are the indicative list where the risk perception of a customer may be considered higher:

I. Customers requesting for frequent change of address/contact details
II. Sudden change in the loan account activity of the customers like frequent excess cash payments.

i) Reliance on third party due diligence

The Company shall, on a need basis, use the services of a third party for due diligence. While using the services of the third party, the Company shall ensure

I. Records or the information of the customer due diligence carried out by the third party is obtained from the third party as per the terms of Service Level Agreement (SLA).
II. Adequate steps are taken by the Company to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
III. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
IV. The third party shall not be based in a country or jurisdiction assessed as high risk.
V. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, shall be with the Company.

j) Risk categorization

The Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorization of customers will be carried out at least once in 6 months. All the customers under different product categories are categorized into low, medium and high risk based on their profile. The Credit manager while appraising the transaction and rendering his approval will prepare the profile of the customer based on risk categorization.

Since Svakarma is into giving term loans to micro enterprises the due diligence done at the time of opening a loan account (detailed earlier in the policy) will be deemed adequate for the tenor of the loan facility. A fresh due diligence will be done if the customer approaches for another loan facility. For SME customers a mid term review will be done.

In case of a change in address, the customer will notify the company for the change in address and provide the necessary documentary proof and the company will update its records.

An indicative categorization for the guidance of businesses is provided in Annexure 1.
Each business process adopts the risk categorization in their respective **credit appraisal memo** subject to confirmation by compliance based on the credit appraisal, customer's background, nature and location of activity, country of origin, sources of funds, client profile, etc.

k) If the Risk Manager believes that the customer needs to be re-categorized into a different risk band, then he may do so by **providing** a justification for the same and getting the approval of the Risk/Business Head.

l) Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. The different business divisions should pay special attention to all complex, unusually large transactions and all unusual patterns that have no apparent economic or visible lawful purpose. Given that the segment the Company is active in is low risk and the facilities offered are term facilities, not in the nature of current or checking accounts and also that its not in the business that involves funds transfer, remittances or cross border transactions, the inherent risk is low and the need for monitoring therefore is minimal

The Company in due course shall put in place an appropriate software application / mechanism to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers.

m) Risk Management

The Company has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

Company's internal audit and compliance functions play a role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function also provides an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements.

Internal Auditors specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

The compliance report is put up before the Board on quarterly intervals.

n) Sharing KYC information with Central KYC Records Registry (CKYCR)

Svakarma shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC guidelines prepared for 'individuals' and 'Legal Entities' as the case may be.

o) Customer Education

The Company may regularly educate the customer of the objectives of the KYC program. The Company on an ongoing basis educates the front desk staff, the branch staff and the new joinees on the elements of KYC, AML & CFT through training programs/e-mail.

p) Applicability of branches and subsidiaries outside India:

The above guidelines shall also apply to the branches.

q) Appointment of designated Director or Principal Officer:

Kalpana Iyer, Managing Director, shall be the Designated Director, responsible for ensuring overall compliance as required under PMLA Act and the Rules. **Meenal Jai Singh, Chief Partnerships Officer** shall be designated as Principal Officer who shall be responsible for furnishing of information to FIU-IND.

Annexure-1
Indicative List for risk categorization

Low Risk Category
Individuals and entities (other than high net worth) whose identities and sources of wealth can be easily identified and transactions in whose accounts conform by and large to the known profile, shall be categorized as low risk. Illustrative examples are:

I. Salaried employees whose salary structure is well-defined
II. People belonging to lower economic strata of the society whose accounts show small balances and low turnover
III. Government departments and Government-owned companies
IV. Statutory bodies & Regulators.

Medium & High-Risk Category
Customers that are likely to pose a higher than average risk may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.
Illustrative examples of medium risk category customers are:

I. Non-Resident customers
II. High Net worth Individuals (individuals with taxable annual income greater than 1 Cr)
III. Trust, charities, NGO's and Organization receiving donations
IV. Companies having close family shareholding or beneficial ownership
V. Firms with 'sleeping partners'

Illustrative examples of high-risk category customers are:

I. Politically Exposed Persons (PEPs) of Indian/Foreign Origin
II. Non face-to-face customers
III. Those with dubious reputation as per public information available
IV. Accounts of bullion dealers and jewelers.

Annexure-2

Customer Identification requirements for Trust/Nominee or Fiduciary Accounts
In the case of any application from trust/nominee or fiduciary accounts, the Company shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary.

In case of any doubt about the persons behind the customer, the Company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons, on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. Company shall take reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

Accounts of companies and firms
Company needs to be vigilant against business entities being used by individuals as a 'front' for transactions. Company should examine the control structure of the entity and identify the natural persons who have a controlling interest and who comprise the management.
These requirements may be moderated according to the risk perception e.g. in the case of a public Company.

Client accounts opened by professional intermediaries
The Company shall not entertain sourcing of accounts through professional intermediaries. However, should the Company engage a Business Correspondent to act on its behalf to identify and /or service customers it will ensure that the Business Correspondent adopts the KYC guidelines as specified by the Company.

Accounts of Politically Exposed Persons (PEPs)
Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/ judicial/ military officers, senior executives of state-owned corporations, important political party officials, etc.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the Company shall obtain the approval of Risk Head and Business Head to continue the business relationship and subject the account to the KYC due diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

Accounts of Resident Outside India
The Company offers products primarily to Indian residents only. The Company if extending any finance to non-residents should check if he is PEP and check all the information available about the person in the public domain. The decision to transact with the PEP should be taken only by the Head of credit of the respective business supported by appropriate verification. The Company is also required to subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the contracts of the family members or close relatives of PEPs.

Identity of Beneficial Owner
The Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client and/or the

person on whose behalf the transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership.

Where the client is a Company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation:
I. "Controlling ownership interest" means ownership of or entitlement to more than twenty five percent (25%) of shares or capital or profits of the Company;
II. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;
(a) where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than fifteen percent (15%) of capital or profits of the partnership;
(b) where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent (15%) of the property or capital or profits of such association or body of individuals;
(c) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;
(d) where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent (15%) or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and
(e) where the client or the owner of the controlling interest is a Company listed on a stock exchange, or is a subsidiary of such a Company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

Accounts of non-face-to-face customers
The Company will not do any transactions with non-face-to-face customers.

Annexure-3

KYC Documents for Identification and verification

Officially Valid Document" (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill)
ii. property or Municipal tax receipt
iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address
iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation

c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above

d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

List of documents required for CIP (Customer Identification Procedure):

For Individuals:

Any one of the documents other than mandatory.
(i) Current valid Passport
(ii) Income Tax PAN card or Form 60 of Income Tax Act, 1962
(iii) Voter's identity card

(iv) valid Driving license
(v) Aadhar Card or letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.
(vi) Central and State Govt. Id Card
(vii) any other officially valid document like job card issued by NREGA duly signed by an officer of the State Government
(viii) Letter issued by a Gazetted officer, with a duly attested photograph of the person (OVD) (should be a photo ID)
(ix) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the company

If Simplified Procedures are applied for verifying the identity of the individual 'low risk' customers, the following documents shall be deemed to be OVD:
1. identity card with applicant's photograph issued by Central/ State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions.
2. Letter issued by a Gazetted officer, with a duly attested photograph of the person.

For Sole Proprietary Firms:

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

In addition to the above CDD, any two of the following documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

a. Registration certificate
b. Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
c. Sales and income tax returns.
d. CST/VAT/ GST certificate (provisional/final).
e. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
g. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.
h. Utility bills such as electricity, water, landline telephone bills, etc.

In cases where the Company is satisfied that it is not possible to furnish two such documents, then the Company may, at its discretion, accept only one of those documents as proof of business/activity.

Provided the Company shall undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

For Partnership firms:

1. Partnership deed (registered, if available)
2. Any officially valid document **(OVD)** identifying the partners and the persons holding the Power of Attorney and their addresses
3. Documents of the person holding an attorney to transact on entity's behalf
   (a) a certified copy of any **OVD** containing details of his identity and address
   (b) one recent photograph
   © the Permanent Account Number or Form No. 60, and
   (d) such other documents pertaining to the nature of business or financial status specified in the KYC policy.

For Companies:

1. Certificate of Incorporation
2. Memorandum and Articles of Association
3. Board resolution and documents of the person holding an attorney to transact on entity's behalf
   (a) a certified copy of any **OVD** containing details of his identity and address
   (b) one recent photograph
   (c) the Permanent Account Number or Form No. 60, and
   (d) such other documents pertaining to the nature of business or financial status specified in the KYC policy.

For Unincorporated Bodies:

Where the customer is an unincorporated association or a body of individuals, the certified copies of the following documents should be obtained:

1. PAN/Form No. 60 of the entity
2. resolution of the managing body of such association or body of individuals
3. power of attorney granted to him to transact on its behalf
4. Permanent Account Number or Form 60 of the persons holding an attorney to transact on its behalf and any OVD for identity and address proof and one recent photograph of such persons.

For Trusts:

1. Trust deed
2. Documents of the person holding an attorney to transact on entity's behalf
   (a) a certified copy of any **OVD** containing details of his identity and address
   (b) one recent photograph
   (c) the Permanent Account Number or Form No. 60, and
   (d) such other documents pertaining to the nature of business or financial status specified in the KYC policy.

For opening accounts of juridical persons not specifically covered above, such as Government or

its departments, societies, universities, and local bodies like village panchayats, one certified copy of the following documents should be obtained:

i. Document showing name of the person authorized to act on behalf of the entity
ii. Officially valid document for proof of identity and address in respect of the person holding an attorney to transact on its behalf and one recent photograph and
iii. Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Illustrative list of activities that would be construed as suspicious transactions

1. Activities that are not consistent with the customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits shall be construed as suspicious transactions.
2. Any attempt to avoid reporting / record-keeping requirements / provides insufficient / suspicious information
3. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
4. Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
5. An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.
6. Certain Employees of the Company arousing suspicion:
    a. An employee whose lavish lifestyle cannot be supported by his or her salary.
    b. Negligence of employees / willful blindness is reported repeatedly.
7. Some examples of suspicious activities/transactions to be monitored:
    a. Multiple accounts under the same name
    b. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.;
    c. There are reasonable doubts over the real beneficiary of the loan
    d. Frequent requests for change of address